UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/763,471	01/22/2004	Daniel G. Wing	2705-320	6671

20575 7590 11/21/2006

MARGER JOHNSON & MCCOLLOM, P.C.
210 SW MORRISON STREET, SUITE 400
PORTLAND, OR 97204

EXAMINER	
GEE, JASON KAI YIN	

ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 11/21/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/763,471	WING, DANIEL G.	
	Examiner	Art Unit	
	Jason K. Gee	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *28 September 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-24* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-24* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *9/28/2006* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This action is response to communication: amendment filed on 09/28/2006.

2. Claims 1-24 are currently pending in this application. Claims 1, 10, and 17 are independent claims. Claims 20-24 are new.

Response to Arguments

Applicant's arguments regarding claims 10-16 have been fully considered but they are not persuasive.

As per claims 10, and 11, the applicants have argued that Edgett does not teach the limitations of the claims. The applicants have argued that Edgett encrypts a password using the password authentication protocol. However, Edgett is not limited to this protocol, as it recites in paragraph 60 that many different protocols may be used. Also, Edgett does not use these protocols to encrypt the password. Edgett uses his own methods for encryption, and it cites in paragraph 64 that the password is compatible with such protocols. Further, the applicant's claimed invention does not explicitly cite transferring video and voice data in the payload in the claims (claims 10 and 11; claim 4 as amended does recite voice data, and thus new art will be applied). Payload data, in its broadest definition, is the bulk of any type of data packet (data not including the header), and may include any type of information, such as password data. Furthermore, Edgett teaches that this invention is applicable to circuit switched networks, as taught in paragraph 84.

As per claim 14, the applicants argue that Schneier does not teach all the limitations of the claims. However, Scheneier in combination with '292 and '092 teaches all the limitations of the claims. Schneier is used to teach a shared key. '292 and '092 teach the devices, such as ingress devices and egress devices, as communication inherently occurs between an egress and an ingress device. A shared key is a key used by two parties, as taught by Schneier. In order to use a key, the users must store the key at least temporarily. This is inherent, as keys cannot be used without being stored. '292 and '092 teaches throughout the reference communicating between the ingress and egress devices.

Applicant's arguments with respect to the remaining claims have been considered but are moot in view of the new ground(s) of rejection.

Drawings

3. The previous objections to the drawings have been withdrawn in response to applicant's amendment.

Claim Rejections - 35 USC § 112

4. The previous 112 rejections regarding claims 4, 5, 7, and 15 have been withdrawn in response to applicant's amendment. The rejection for claim 6 and 12 still remains.

5. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

6. Claims 1-9, 17-19, and 20-23 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

As per claims 1-9, 17-19, and 20-23, the applicants recite limitations that are not explicitly cited in the specification. Limitations such as "encrypted layer four transport layers", "layer three network layer headers", "lower layer header", "transport layer headers", and "network layer headers" are not labeled as such in the specification. It is not clear whether other terms are used in the specification to teach the layering of the headers. The specification discusses only headers in general, and does not go into detail the layering of the headers. Also, encrypting transport layer headers while replacing a certain layer of header without replacing other layers of the header is not taught throughout the specification.

7. Claims 1-9, 17-19, and 20-22 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to enable one

skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention.

As per claims 1-9, 17-19, and 20-22, the applicants recite limitations such as "encrypted layer four transport layers", "layer three network layer headers", "lower layer header", and "transport layer headers". The layering of data packets and headers are not mentioned in the applicant's specification, and it is not enabled in the art how to make use of the layering of the headers and packets.

8. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

9. Claims 1-9 and 17-19 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

As per claim 6, the claim recites the limitation "the identified non-supporting egress devices." There is insufficient antecedent basis for this limitation in the claim.

As per claim 12, the claim in which this claim is dependent on (claim 10) teaches that IP packet payloads are not decrypted. It is unclear in claim 12 why there are some "other IP packet payloads" that are decrypted. It is not clear why a processor would forward IP packet payloads that are decrypted when the processor deals with sending and forwarding packets unencrypted. By claiming forwarding decrypted packets and encrypted packets, the applicants are claiming forwarding any type of packet, in which any reference that teaches sending packets will apply as relevant art.

As per claims 1-9 and 17-19, the applicants recite limitations such as "encrypted layer four transport layers", "layer three network layer headers", "lower layer header", and "transport layer headers". It is not clear which layer The layering of data packets and headers are not mentioned in the applicant's specification, and it is not enabled in the art how to make use of the layering of the headers and packets.

Claim Rejections - 35 USC § 103

10. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

11. Claims 1-3 are rejected under 35 U.S.C. 103(a) as being anticipated by Focsaneanu et al. US Patent No. 5,991,292 (hereinafter '292), and in view of Matsuhira US Patent Application Publication 2004/0205359 (hereinafter '359).

As per claim 1, Focsaneanu '292 teaches a method of transporting encrypted media, comprising: receiving a request (col. 6 lines 18-27 and Figure 5) to transport encrypted (col. 16 lines 1-17) Internet Protocol (IP) media packets over a circuit switched network (Figure 5); establishing an IP link over the circuit switched network

(col. 7 lines 29-67); and transporting the encrypted IP media packets over the IP link established over the circuit switched network (Figure 5, where packets are transferred from the terminals to the PSTN).

However, '292 does not explicitly teach the details of the layering of packets and headers. As best understood by the Examiner, the newly amended limitations and encrypting layers of packets in header information is taught throughout '359, such as in paragraphs 116, 117, 120, 197, and 203.

At the time of the invention, it would have been obvious to include encrypting headers in accordance with layers. One of ordinary skill in the art would have been motivated to perform such an addition to secure security. '359 teaches this in paragraph 26, by using packet filtering with VoIP technology. '359 is relevant art, as it teaches VoIP, which is well known in the art and deals with sending data from circuit switched networks to packet-switched networks.

As per claim 2, Focsaneanu '292 teaches establishing a data channel over the circuit switched network and using a Point to Point Protocol over the data channel to establish the IP link (col. 16 lines 1-17).

As per claim 3, Focsaneanu '292 teaches establishing a data channel over an ISDN channel of a Public Services Telephone Network (col. 16 lines 1-17 and also Figures 16 and 17).

12. Claims 1-3, 5, and 17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Voit et al. US Patent No. 6,137,869 (hereinafter '137), and in view of Matsuhira US Patent Application Publication 2004/0205359 (hereinafter '359).

As per claim 1, Voit '869 teaches a method of transporting encrypted media, comprising: receiving a request to transport encrypted Internet Protocol (IP) media packets over a circuit switched network (col. 5 lines 48-62, Figure 1B); establishing an IP link over the circuit switched network (Figure 1B, col. 10 lines 59-64); and transporting the encrypted IP media packets over the IP link established over the circuit switched network (col. 5 lines 47-61, col. 10 lines 59-64, and also inherent that these packets are sent through the established IP link).

However, '869 does not explicitly teach the details of the layering of packets and headers. As best understood by the Examiner, the newly amended limitations and encrypting layers of packets in header information is taught throughout '359, such as in paragraphs 116, 117, 120, 197, and 203.

As per claim 2, 'Voit '869 teaches establishing a data channel over the circuit switched network and using a PPP over the data channel to establish the link (col. 10 lines 59-64).

As per claim 3, Voit '869 teaches establishing the data channel over an ISDN channel of a PSTN (col. 14 lines 30-37).

As per claim 5, Voit '869 teaches receiving call requests from endpoints connected to the packet switched network (Figure 1B, showing connections with the packet and circuit switched network with ITG 118, and Figure 2 showing the details of the connections, described in col. 9 lines 11-53); identifying the call requests that require IP encryption (inherent has it identifies all call requests, and encryption is shown in col. 9 lines 35-53); identifying ingress devices in the circuit switched network associated with the identified call requests that support transport of the encrypted IP media packets over the circuit switched network (col. 9 lines 35-53); establishing IP links over the circuit switched network with the identified egress devices (col. 10 lines 60-65); and transporting the encrypted IP media packets to the identified ingress devices (inherent and taught throughout the reference, as the ingress devices are connected to the Internet and packets are exchanged during communications after they are connected; col. 9 line 35 to col. 10 line 40).

Independent claim 17 is rejected using the same basis of arguments used to reject claims 1, 2, 3, and 5 above, as all the elements contained in claim 17 are included in claims 1, 2, 3, and 5. As best understood by the Examiner, the newly amended limitations and encrypting layers of packets in header information is taught throughout '359, such as in paragraphs 116, 117, 120, 197, and 203.

13. Claim 4 is rejected under 35 U.S.C. 103(a) as being unpatentable over Edgett '092 and Matsuhira '359 as applied above, and further in view of Torvinen US Patent Application Publication 2003/0021415 (hereinafter '415).

As per claim 4, '092 teaches transporting encrypted IP media packets over a packet switched network without decrypting or decoding the media that includes voice data (paragraph 19).

At the time of the invention, it would have been obvious to one of ordinary skill in the art to combine the teachings of '415 with '092 and '359. Sending data without decrypting it would increase the speed and would ensure security, as described in paragraph 19.

14. Claim 4 is rejected under 35 U.S.C. 103(a) as being unpatentable over Voit '869 and Matsuhira '359 as applied above, and further in view of Torvinen US Patent Application Publication 2003/0021415 (hereinafter '415).

As per claim 4, '869 teaches transporting encrypted IP media packets over a packet switched network without decrypting or decoding the media that includes voice data (paragraph 19).

At the time of the invention, it would have been obvious to one of ordinary skill in the art to combine the teachings of '415 with '869 and '359. Sending data without decrypting it would increase the speed and would ensure security, as described in paragraph 19.

15. Claims 10, and 11 are rejected under 35 U.S.C. 103(a) as being unpatentable over Voit '869 as applied above, and in view of Edgett et al. US Patent Application Publication 2003/0056092 (hereinafter '092).

As per claim 4, Voit '869 does not explicitly teach including transporting the encrypted IP media packets over the packet switched network without decrypting or decoding the media in the encrypted IP media packets. However, this is taught in Edgett '092. As can be seen in Figure 2 and paragraphs 65 and 66, the encrypted media packets are sent through the packet switched network and are decrypted only after It passes through the packet switched network into the network decryption server.

As per independent claim 10, Voit '869 teaches a network processing device, comprising: a processor configured to establish a connection between two endpoints that extends over an Internet Protocol (IP) network and a circuit switched network (Figure 1B), the processor forwarding packets having an encrypted IP packet payload between the two endpoints (col. 5 lines 48-61). However, Voit does not explicitly teach wherein the packet payload is not decrypted when transferred between the IP network and circuit switched network. However, this is taught in Edgett '092. As can be seen in Figure 2 and paragraphs 65 and 66, the encrypted media packets are sent through the packet switched network and are decrypted only after it passes through the packet switched network into the network decryption server. These packets are not decrypted between the packet and circuit switched communication.

At the time of the invention, it would have been obvious to one of ordinary skill in the art to include sending packets over a packet switched network without decrypting or decoding the media. One of ordinary skill in the art would have been motivated to perform such an addition to increase security by not sending out critical information which is unencrypted. This is taught in '092 in paragraph 13-16, where it teaches that this invention wants to improve on the ability to send out critical information in packets which is encrypted.

As per claim 11, 'Voit '869 teaches wherein the processor establishes an IP link over the circuit switched network and forwards the encrypted IP packet payload over the IP link (col. 10 lines 59-64).

16. Claims 6, 7, and 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Voit '869 and Matsuhira '359 as applied above, and further in view of Bulfer et al. US Patent No. 5,392,357 (hereinafter '357).

As per claim 6, Voit '869 and Matsuhira '359 teaches all the limitations in the previous claims, but does not explicitly teach the limitations of claim 6. However, Bulfer '357 teaches identifying non-supporting ingress devices in circuit switched network associated with the identified call requests that do not support transport of encrypted IP media packets over the circuit switched network (col. 12 line 23 to col. 13 line 34); establishing circuit switched connections over the circuit switched network for the identified non-supporting egress devices (col. 12 line 23 to col. 13 line 34 where

connections are established in order to decode/encode); decrypting and decoding media in the encrypted IP media packets associated with the non-supporting ingress devices (col. 12 line 23 to col. 13 line 34); and re-encoding and re-encrypting the media into a circuit switched network format; and transporting the re-encoded and re-encrypted media over the circuit switched connections to the non-supporting egress devices (col. 12 line 23 to col. 13 line 34). (Also, this is all summed up in the summary in (col. 2 lines 5-15, also seen in Figure 1).

At the time of the invention, it would have been obvious to one of ordinary skill in the art to include decoding/decrypting media and reencoding/reencrypting in a circuit switched network. One of ordinary skill in the art would have been motivated to perform such an addition to allow flexibility so that different parties may engage in secure communications with one another. This is taught in '357 in col. 1 lines 30-38, where it cites "present security techniques have several limitations, including the general requirement that both the calling and called parties that desire to engage in a secure communication must have compatible security equipment that can send and receive encrypted signals using common handshaking protocols and encryption algorithms. If this is not the case, secure communications are normally not possible." It goes on in col. 2 lines 26-30 to teach "The invention also permits secure communication between parties using security devices with different handshaking protocols and encryption algorithms."

As per claim 7, Voit '869 teaches all the limitations of the previous claims, but does not explicitly teach the specifics of key exchange taught in claim 7. However, this

is taught in '357 in col. 12 line 50 to col. 14 line 14. The training mentioned in these passages deal with key exchange, which is taught in col. 8 lines 26-44.

As per claim 18, Voit '869 teaches authenticating the identified call requests with ingress gateways (col. 5 lines 44-61) and conducing PPP sessions with the ingress gateways when the ingress gateways are authenticated (col. 10 lines 60-64). Exchanging encryption keys are taught in Bulfer '357 in col. 8 lines 27-44.

17. Claim 8 is rejected under 35 U.S.C. 103(a) as being obvious over Voit '869 and Matsuhira '359.

As per claim 8, Voit '869 teaches encrypting the media packets (col. 5 lines 48-62), but does not explicitly teach encrypting and decrypting the packets only once. However, the Examiner asserts that this would be obvious. One of ordinary skill in the art would have been motivated to encrypt/decrypt packets only once, as it provides security, and it saves time compared to encrypting/decrypting more than once.

18. Claim 9 is rejected under 35 U.S.C. 103(a) as being unpatentable over Voit '869 and Matsuhira '359 as applied above, and further in view of Lindholm et al. US Patent Application Publication 2004/0019801 (hereinafter '801).

As per claim 9, Voit '869 teaches the utilizing PPP and ISDN in (col. 10 lines 59-64 and col. 14 lines 30-37), but does not explicitly teach using SRTP. However, this is taught in Lindholm '801 in paragraph 26.

At the time of the invention, it would have been obvious to one of ordinary skill in the art to utilize SRTP. One of ordinary skill in the art would have been motivated to perform such an addition to provide confidentiality and protection of the user. This is taught in paragraph 26, where it cites "An example of such a cryptographic mechanism is the Secure Real-time Transport Protocol (SRTP), which can provide both confidentiality protection of the user data and integrity protection on a per packet basis."

19. Claim 19 is rejected under 35 U.S.C. 103(a) as being unpatentable over Voit '869 in view of Bulfer '357 as applied above, and further in view of Bruce Schneier's *Applied Cryptography* (2nd Edition).

As per claim 19, the Voit and Bulfer combination teaches all the limitations of the previous claims, but does not explicitly teach encrypting the encryption keys using shared keys and sending the encrypted encryption key to the ingress gateways. However, Schneier teaches encrypting keys using shared keys and sending the encrypted keys out. This is taught on pages 47 and 48.

At the time of the invention, it would have been obvious to one of ordinary skill in the art to include encrypted key exchange in a circuit switched network. One of ordinary skill in the art would have been motivated to perform such an addition to allow flexibility so that different parties may engage in secure communications with one another. This is taught in '357 in col. 1 lines 30-38, where it cites "present security techniques have several limitations, including the general requirement that both the calling and called parties that desire to engage in a secure communication must have compatible security

equipment that can send and receive encrypted signals using common handshaking protocols and encryption algorithms. If this is not the case, secure communications are normally not possible." It goes on in col. 2 lines 26-30 to teach "The invention also permits secure communication between parties using security devices with different handshaking protocols and encryption algorithms."

20. Claims 10 and 11 are rejected under 35 U.S.C. 103(a) as being unpatentable over Focsaneanu '292 as applied above, and in view of Edgett et al. US Patent Application Publication 2003/0056092 (hereinafter '092).

As per claim 4, Focsaneanu does not explicitly teach including transporting the encrypted IP media packets over the packet switched network without decrypting or decoding the media in the encrypted IP media packets. However, this is taught in Edgett '092. As can be seen in Figure 2 and paragraphs 65 and 66, the encrypted media packets are sent through the packet switched network and are decrypted only after It passes through the packet switched network into the network decryption server.

As per independent claim 10, Focsaneanu teaches a processor configured to establish a connection between two endpoints that extends over an Internet Protocol network and a circuit switched network (Figure 8), the processor forwarding packets having an encrypted IP packet payload between the two endpoints (col. 16 lines 1-17). However, Focsaneanu does not explicitly teach that the encrypted IP packets are not

decrypted when transferred between the IP network and circuit switched network. However, this is taught in Edgett '092. As can be seen in Figure 2 and paragraphs 65 and 66, the encrypted media packets are sent through the packet switched network and are decrypted only after it passes through the packet switched network into the network decryption server. These packets are not decrypted between the packet and circuit switched communication.

At the time of the invention, it would have been obvious to one of ordinary skill in the art to include sending packets over a packet switched network without decrypting or decoding the media. One of ordinary skill in the art would have been motivated to perform such an addition to increase security by not sending out critical information which is unencrypted. This is taught in '092 in paragraph 13-16, where it teaches that this invention wants to improve on the ability to send out critical information in packets which is encrypted.

As per claim 11, Focsaneanu teaches wherein the processor establishes an IP link over the circuit switched network and forwards the encrypted IP packet payload over the IP link (col. 16 lines 1-17).

21. Claim 9 is rejected under 35 U.S.C. 103(a) as being unpatentable over Focsaneanu '292 and Matsuhira '359 as applied above, and further in view of Lindholm et al. US Patent Application Publication 2004/0019801 (hereinafter '801).

As per claim 9, Focsaneanu '292 teaches the utilizing PPP and ISDN in (col. 16 lines 1-17), but does not explicitly teach using SRTP. However, this is taught in Lindholm '801 in paragraph 26.

At the time of the invention, it would have been obvious to one of ordinary skill in the art to utilize SRTP. One of ordinary skill in the art would have been motivated to perform such an addition to provide confidentiality and protection of the user. This is taught in paragraph 26, where it cites "An example of such a cryptographic mechanism is the Secure Real-time Transport Protocol (SRTP), which can provide both confidentiality protection of the user data and integrity protection on a per packet basis."

22. Claim 12 is rejected under 35 U.S.C. 103(a) as being unpatentable over Focsaneanu '292 and in view of Edgett '092 as applied above, and further in view of obviousness over Saadat et al. US Patent Application Publication 2005/0125357 (hereinafter '357.

As per claim 12, Focsaneanu teaches the use of Codec, as can be seen in Figures 8 and 14, but the Focsaneanu and Edgett combination does not explicitly teach compressing a non-decrypted data at a higher compression rate using a second codec. However, compressing data at different rates due to encryption or decryption is taught in Saadat in paragraph 80.

At the time of the invention, it would have been obvious to one of ordinary skill in the art to compress data using different codecs. One of ordinary skill in the art would have been motivated to perform such an addition allow more efficiency when storing or

transporting material by compressing materials at different compression rates. This is taught in paragraphs 11 and 12, where it teaches that the new invention would overcome the old art by providing a cheaper and better way to store video without lowering video quality.

23. Claim 13 is rejected under 35 U.S.C. 103(a) as being unpatentable over Focsaneanu '292 and in view of Edgett '092 as applied above, and further in view of Bowman-Amuah US Patent No. 6,426,948 (hereinafter '948).

As per claim 13, the '292 and '092 combination does not explicitly teach identifying phone numbers that can be transferred between the IP network and the circuit switched network without decrypting the encrypted IP packets payload. However, Bowman-Amuah '948 teaches storing up phone numbers in col. 39 lines 20-30.

At the time of the invention, it would have been obvious to one of ordinary skill in the art to include a memory containing a dial plan for identifying phone numbers. One of ordinary skill in the art would have been motivated to perform such an addition to allow easy access to those who use the system regularly. This is taught in col. 39 lines 19-22: "For callers that utilize the callback system on a regular basis a custom profile is provided as an extension to the users existing profile information.

24. Claim 14 is rejected under 35 U.S.C. 103(a) as being unpatentable over Focsaneanu '292 and in view of Edgett '092 as applied above, and further in view of Bruce Schneier's *Applied Cryptography* (2nd Edition).

As per claim 14, '292 and '092 does not explicitly teach receiving a first key from a first endpoint, encrypting the first key using the shared key and sending the encrypted first key to the ingress device. However, this is taught in Schneier on page 48. (Memory for storing a key is inherent as it uses the key).

At the time of the invention, it would have been obvious to one of ordinary skill in the art to incorporate the use of Key Exchange in a secure hybrid system of circuit and packet switched networks. One of ordinary skill in the art would have been motivated to perform such an addition to allow easy security use. This is taught by Schneier on page 48, where it cites "In some practical implementations, both Alice's and Bob's signed public keys will be available on a database. This makes the key-exchange protocol even easier, and Alice can send a secure message to Bob even if he has never heard of her."

25. Claim 15 is rejected under 35 U.S.C. 103(a) as being unpatentable over Focsaneanu '292 and in view of Edgett '092 and Schneier, and further in view of being obvious over Bulfer et al US Patent No. 5,392,357 (hereinafter '357).

As per claim 15, the '292 combination does not explicitly teach the limitations of claim 15, but Bulfer teaches this in col. 12 line 50 to col. 14 line 14. The training mentioned in these passages deal with key exchange, which is taught in col. 8 lines 26-

44. Shared keys are used to decrypt keys, as taught by Schneier, and it would have been obvious to one of ordinary skill in the art to decrypt more than one key using the shared key. As can be seen, Bulfer teaches a plurality of keys, and it would be useful to have multiple keys for more security.

At the time of the invention, it would have been obvious to one of ordinary skill in the art to include key exchange in a circuit switched network. One of ordinary skill in the art would have been motivated to perform such an addition to allow flexibility so that different parties may engage in secure communications with one another. This is taught in '357 in col. 1 lines 30-38, where it cites "present security techniques have several limitations, including the general requirement that both the calling and called parties that desire to engage in a secure communication must have compatible security equipment that can send and receive encrypted signals using common handshaking protocols and encryption algorithms. If this is not the case, secure communications are normally not possible." It goes on in col. 2 lines 26-30 to teach "The invention also permits secure communication between parties using security devices with different handshaking protocols and encryption algorithms."

26. Claim 16 is rejected under 35 U.S.C. 103(a) as being unpatentable over Focsaneanu '292 and in view of Edgett '092 as applied above, and further in view of Lindholm et al. US Patent Application Publication 2004/0019801 (hereinafter '801).

As per claim 16, Focsaneanu '292 teaches the utilizing PPP and ISDN in (col. 16 lines 1-17), but the combination does not explicitly teach using SRTP. However, this is taught in Lindholm '801 in paragraph 26.

At the time of the invention, it would have been obvious to one of ordinary skill in the art to utilize SRTP. One of ordinary skill in the art would have been motivated to perform such an addition to provide confidentiality and protection of the user. This is taught in paragraph 26, where it cites "An example of such a cryptographic mechanism is the Secure Real-time Transport Protocol (SRTP), which can provide both confidentiality protection of the user data and integrity protection on a per packet basis."

27. Claims 20-22 are rejected under 35 U.S.C. 103(a) as being anticipated by Rogers et al. US Patent No. 7,110,391 (hereinafter '391), and in view of Ofek et al. US Patent Application Publication 2001/0038628 (hereinafter '628).

As per claim 20, Rogers '391 teaches an apparatus comprising: one or more processors and a memory coupled to the processors comprising instructions executable by the processors, the processors operable when executing the instructions to (inherent to the '391 reference in order for it to work, discussed in col. 4 lines 56 to 68, where data network includes applications such as web browsing, mail transfer, etc, which require a processor and memory); receive packets over a packet switched network, the packets having first and second headers excluded from encryption for a payload (Figure 3b, col. 5 line 63 to col. 6 line 4); format the first and second headers without decrypting

the encryption for the third header and the payload (col. 5 lines 47-55 and 59-65; col. 10 lines 38-45 (where adding information to headers is formatting) ; col. 12 lines 6-8); a payload remaining encrypted during transfer between the endpoints (Figure 3b; col. 6 lines 4-22, where interface card 16 is part of telephonic device 18, such as shown in Figure 2 and described in col. 4 lines 1-8);establish a connection over a circuit switched network to a remote network device (Figure 3b, where data network is remote); send the packets having the encrypted payload on the connection over the circuit switched network (Figure 3b).

However, at the time of the invention, '391 does not explicitly teach encrypting the third header. The encryption of headers is well known in the art, and is taught throughout Ofek '628, such as in paragraph 3.

At the time of the invention, it would have been obvious to one of ordinary skill in the art to encrypt headers. One of ordinary skill in the art would have been motivated to perform such addition to increase security, as vital information may be located inside header information. Encrypting headers to increase security features are important, and is taught in paragraph 3 of '628.

As per claim 21, '391 teaches that the first and second hers are IP and UDP headers (Figure 3B and taught throughout the reference). '628 teaches encrypted RTP headers, such as in paragraph 10, 15, 86, and Figure 4.

As per claim 22, '391 teaches wherein the encrypted payload includes voice data (col. 3 lines 41-56) such that the voice data is securely transported across both the

circuit switched network and the packet switched network without intermediary decryption (no intermediary decryption, as rejected in claim 20 above, where the payload (voice data) remains encrypted during transfer between endpoints).

28. Claim 23 is rejected under 35 U.S.C. 103(a) as being anticipated by Rogers et al. US Patent No. 7,110,391 (hereinafter '391), and in view of Hluchyj US Patent No. 6,381,238 (hereinafter '238).

As per clam 23, '391 teaches a network processing device, comprising: a processor configured to establish a connection between two endpoints that extends over an Internet Protocol (IP) network and a circuit switched network (Figure 3b, wherein a processor is inherent, as can be seen in the rejection for claim 20), the processor forwarding packets having an encrypted IP packet payload between the two endpoints without decrypting the encrypted IP packet payload when transferred between the IP network and circuit switched network (Figure 3b, col. 4 lines 1-9; col. 5 line 42 to col. 6 line 23; also see rejection for claim 20); the network processing device is configured to identify one or more network layer headers included in the packets (col. 5 line 42 to col. 6 line 23, wherein headers must be identified in order to be processed); preserving encryption on a corresponding payload (Figure 3B; col. 6 lines 1-20); locally generate one or more network layer headers (col. 12 lines 5-10); forward the packets having the locally generated headers and the encrypted corresponding payload over the

connection (Figure 3B). '628 teaches that headers ((transport layer header in this case) may be encrypted, as taught in paragraph 3.

However, at the time of the invention, '391 does not explicitly teach removing network layer headers. Hluchyj '238 teaches this though, in col. 5 lines 49-55. The packet adaptation would remove the necessary headers, add new ones, and preserve the old ones if necessary. As can be seen, all these subcomponents may be regrouped and reordered, and would be sent as a packet. The combination of these three references teaches all the limitations of the claim.

At the time of the invention, it would have been obvious to combine the teachings of '391 and '628 with '238. One of ordinary skill in the art would have been motivated to perform such an addition to allow flexibility of a packet switch fabric while reducing the cost and complexity of the system (col. 2 lines 5-11).

29. Claim 24 is rejected under 35 U.S.C. 103(a) as being anticipated by '391 and '238 as applied above, and further in view Seshadri et al. US Patent Application Publication 2004/0068481 (hereinafter '481), and further in view of Bulfer '357.

As per claim 24, 391 teaches a network processing device, comprising: a processor configured to establish a connection between two endpoints that extends over an Internet Protocol (IP) network and a circuit switched network (Figure 3b, wherein a processor is inherent, as can be seen in the rejection for claim 20), the processor forwarding packets having an encrypted IP packet payload between the two

endpoints without decrypting the encrypted IP packet payload when transferred between the IP network and circuit switched network (Figure 3b, col. 4 lines 1-9; col. 5 line 42 to col. 6 line 23; also see rejection for claim 20).

However, at the time of the invention, '391 does not explicitly teach receiving an out-of-band communication that provides a secret that is shared. However, this is taught in Seshadri '481 in paragraph 169.

At the time of the invention, it would have been obvious to one of ordinary skill in the art to include the teachings of Seshadri with '391. One of ordinary skill in the art would have been motivated to perform such an addition to provide more security, as out-of-band channels are well known in the art to provide secure transactions between parties.

Claim 24 also claims a method of key exchange and the use of a gateway. All the limitations of the key exchanging process and the gateway are taught in 'Bulfer '357, in col. 12 line 50 to col 14. line 15.

At the time of the invention, it would have been obvious to one of ordinary skill in the art to include the encrypting/decrypting key exchange in a circuit switched/packet-switch network. One of ordinary skill in the art would have been motivated to perform such an addition to allow flexibility so that different parties may engage in secure communications with one another. This is taught in '357 in col. 1 lines 30-38, where it cites "present security techniques have several limitations, including the general requirement that both the calling and called parties that desire to engage in a secure communication must have compatible security equipment that can send and receive

encrypted signals using common handshaking protocols and encryption algorithms. If this is not the case, secure communications are normally not possible." It goes on in col. 2 lines 26-30 to teach "The invention also permits secure communication between parties using security devices with different handshaking protocols and encryption algorithms."

Conclusion

30. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

31. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jason K. Gee whose telephone number is (571) 272-6431. The examiner can normally be reached on M-F, 7:00 am to 4:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jacques Louis-Jacques can be reached on (571) 272-38386962. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Jason Gee
Patent Examiner
Technology Center 2134
11/14/06

GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100